1. Record Nr.	UNISA996465473403316
Titolo	Information Security Applications [[electronic resource]] : 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers / / edited by Chae Hoon Lim, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 472 p.)
Collana	Security and Cryptology ; ; 3325
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Operating systems (Computers) Algorithms Computer networks Electronic data processing—Management Computers, Special purpose Cryptology Operating Systems Computer Communication Networks IT Operations Special Purpose and Application-Based Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Network/Computer Security -- Impacts of Security Protocols on Real-Time Multimedia Communications -- An Improvement on Privacy and Authentication in GSM -- Encrypted Watermarks and Linux Laptop Security -- Inconsistency Detection of Authorization Policies in Distributed Component Environment -- Public Key Schemes I -- Custodian-Hiding Verifiable Encryption -- Proving Key Usage -- Public Key Encryption with Conjunctive Field Keyword Search -- Intrusion Detection I -- A Probabilistic Method for Detecting Anomalous Program Behavior -- Service Discrimination and Audit File Reduction for Effective

Intrusion Detection -- IDS False Alarm Filtering Using KNN Classifier -- Watermarking/Anti-spamming -- Content-Based Synchronization Using the Local Invariant Feature for Robust Watermarking -- Some Fitting of Naive Bayesian Spam Filtering for Japanese Environment -- Public Key Schemes II -- Efficient Authenticated Key Agreement Protocol for Dynamic Groups -- A Ring Signature Scheme Using Bilinear Pairings -- Verifiable Pairing and Its Applications -- Intrusion Detection II -- Improving the Performance of Signature-Based Network Intrusion Detection Sensors by Multi-threading -- An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks -- Application of Content Computing in Honeyfarm -- Digital Rights Management -- License Protection with a Tamper-Resistant Token -- An Adaptive Approach to Hardware Alteration for Digital Rights Management -- Dynamic Fingerprinting over Broadcast Using Revocation Scheme -- Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels -- e-Commerce Security -- Vulnerability of a Mobile Payment System Proposed at WISA 2002 -- Fair Offline Payment Using Verifiable Encryption -- A Limited-Used Key Generation Scheme for Internet Transactions -- Efficient Implementation -- Efficient Representation and Software Implementation of Resilient Maiorana-McFarland S-boxes -- Signed Digit Representation with NAF and Balanced Ternary Form and Efficient Exponentiation in GF(q n) Using a Gaussian Normal Basis of Type II -- Novel Efficient Implementations of Hyperelliptic Curve Cryptosystems Using Degenerate Divisors -- Hyperelliptic Curve Coprocessors on a FPGA -- Anonymous Communication -- Key-Exchange Protocol Using Pre-agreed Session-ID -- A New k-Anonymous Message Transmission Protocol -- Onions Based on Universal Re-encryption – Anonymous Communication Immune Against Repetitive Attack -- Side-Channel Attacks -- Side Channel Cryptanalysis on SEED -- Secure and Efficient AES Software Implementation for Smart Cards -- Practical Template Attacks -- Evaluation and Improvement of the Tempest Fonts.

Sommario/riassunto

The 5th International Workshop on Information Security Applications (WISA 2004) was held in Jeju Island, Korea during August 23-25, 2004. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC). The aim of the workshop is to serve as a forum for new conceptual and - perimental research results in the area of information security applications from the academic community as well as from the industry. The workshop program covers a wide range of security aspects including cryptography, cryptanalysis, network/system security and implementation aspects. The programcommittee received169 papersfrom 22 countries,andaccepted 37 papers for a full presentation track and 30 papers for a short presentation track. Each paper was carefully evaluated through peer-review by at least three members of the programcommittee. This volume contains revised versions of 36 papers accepted and presented in the full presentation track. Short papers were only published in the WISA 2004 pre-proceedings as preliminary versions and are allowed to be published elsewhere as extended versions. In addition to the contributed papers, Professors Gene Tsudik and Ross Andersongaveinvitedtalks, entitledSecurityinOutsourcedDatabasesandWhat does ‘Security’ mean for Ubiquitous Applications?, respectively.